Journal of Number Theory 129 (2009) 2072–2092

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Minimal resolution of Atkin–Lehner quotients of $X_0(N)$

Hui Xue

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

ARTICLE INFO

Article history:
Received 23 September 2008
Revised 30 January 2009
Available online 15 May 2009
Communicated by S.J. Edixhoven

MSC:
11G18

ABSTRACT

Let $X_0(N)$ be the classic modular curve of level N over $\mathbb{Z}$. Let W_M be the Atkin–Lehner involution of $X_0(N)$ associated to a divisor M with $(M, N/M) = 1$. In this paper an explicit description is given for the minimal resolution over $\mathbb{Z}[1/6]$ of the Atkin–Lehner quotient $X_0(N)/W_M$. As an application a new proof of Deuring's formula on the number of supersingular j-invariants in $\mathbb{F}_p$ is given. In certain cases it is also shown that the action of Hecke operators on the component group of the Jacobian of the Atkin–Lehner quotient is Eisenstein.

1. Introduction

Throughout the paper the letter p denotes a prime greater than 3 and $N = p^n N'$ is a positive integer with $(p, N') = 1$ and $n \geqslant 1$. To simplify some arguments (see Section 3), we assume that the exponent of 2 in N is not 1 or 2, and that the exponent of 3 in N is not 1. Let $[\Gamma_0(N)]$ be the moduli stack of elliptic curves (E, C_N) with an N-cyclic subgroup C_N [11, Section 3.4], or equivalently isogenies $(\varphi : E \to E')$ with an N-cyclic kernel. Let $M > 1$ be a factor of N such that $(M, N/M) = 1$. Associated to M is the Atkin–Lehner involution, denoted W_M, whose action on $[\Gamma_0(N)]$ is given by

$$W_M : \big[(E, C_N)\big] \mapsto \big[\big(E/C_M, (C_N + E[M])/C_M\big)\big].$$

This action naturally induces an involution on the coarse moduli space $Y_0(N)$ of $[\Gamma_0(N)]$ and its compactification $X_0(N)$ [11], denoted again by W_M. The Atkin–Lehner quotient is the quotient scheme $X_0^M(N) = X_0(N)/W_M$ with respect to W_M. This Atkin–Lehner quotient in general is not regular. In this paper we will locate the singularities of $X_0^M(N)$, and give an explicit description of special fibers of its minimal resolution over $\overline{\mathbb{F}}_p$, see [12, Chapter 9] for general facts on resolution of arithmetic curves.

E-mail address: huixue@clemson.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.02.020

Our computation is similar to Edixhoven's work [4] on the resolution of singularities of $X_0(N)$. The difference is that [4] uses the explicit description of local equations of $[\Gamma_0(N)]$, hence is able to obtain the explicit local equations for the resolution, while we do not use or write down the explicit local equations (for we do not know the explicit local action of W_M). Instead, we use the general theory developed in Sections 2 through 4 to extract information on the resolution. These information are sufficient to determine the global configuration of the minimal resolution in Section 5.

The main motivation of our consideration of the curve $X_0^M(N)$ comes from the paper [7] by Gross, Kohnen and Zagier. In that paper intersection numbers of certain CM points on $X_0^N(N)$ are computed, and the minimal resolution of $X_0^N(N)$ is briefly addressed. Readers may also find another application of the curve $X_0^p(p)$ in Jao's paper [9].

Now let us briefly describe the basic idea of our approach. First we observe that the involution W_M extends naturally onto the minimal resolution $\widetilde{X}_0(N)$ of $X_0(N)$. So we only need to study some basic properties of an involution on a two dimensional regular local scheme. In Section 2 we will see there are essentially two cases: one produces a singular quotient and the other one gives a regular quotient. The resolution of the quotient singularity is accomplished by just one blowing up. In this section we also give a regular system of local parameters of $[\Gamma_0(N)]$ at certain ordinary points (Lemma 2.3), thus supplement a related result of [11, Proposition 7.8.2] at supersingular points. Such a system of parameters has been used in [4] without any proof.

In Section 3 we determine the points on $X_0(N)$ that do produce singularities on the Atkin–Lehner quotient $X_0^M(N)$. Then in Section 4 we resolve locally all the singularities found in Section 3.

In Section 5 we put together the local results of Section 4, and give a scheme that provides the global configuration of the special fiber $\widetilde{X}_0^M(N)_{\overline{\mathbb{F}}_p}$ of the minimal resolution, such as the reduced irreducible components, their multiplicities and their local intersection numbers.

In Section 6 we carry out the scheme outlined in Section 5 for the special cases $N = p$ and p^2.

In Section 7 two applications are given. The first one is to supply a new proof of Deuring's formula on the number of $\mathbb{F}_p$-rational supersingular j-invariants. In the second application we study the action of Hecke operators on the component group of the Jacobian of $X_0^M(N)$, and show in certain cases that these Hecke actions are Eisenstein.

The following is a list of notation and assumption that will be used throughout the paper.
For any number N with $p^n \parallel N$ we write $N' = N/p^n$. (Ell/R) denotes the modular stack of elliptic curves over R-schemes.
$[\Gamma_0(N)]$ denotes the moduli problem that assigns to an elliptic curve E the set of Drinfeld cyclic N-subgroups of E, or equivalently the set of N-cyclic isogenies between elliptic curves.
The (a, b)-component (of $[\Gamma_0(N)]$ over $\mathbb{F}_p$) is the reduced coarse moduli scheme parameterizing $[(E, C_{N'}, C_{p^n})]$ where C_{p^n} is an (a, b)-cyclic subgroup of E (in the sense of [11]).
$\widetilde{X}_0(N)$ denotes the minimal resolution of $X_0(N)$ constructed in [4].
$X_0^M(N)$ denotes the Atkin–Lehner quotient of $X_0(N)$ with respect to W_M, and $\widetilde{X}_0^M(N)$ denotes the minimal resolution of $X_0^M(N)$.

2. Some local properties of involutions

In this section let $(R, \mathfrak{m})$ be a complete noetherian regular local ring of dimension two. Let $p \neq 2$ be the characteristic of the algebraically closed residue field $k = R/\mathfrak{m}$, and let W be an involution on R that acts trivially on the residue field k.

Lemma 2.1. *With the above notation and assumption, if the induced action of W on the cotangent space $\mathfrak{m}/\mathfrak{m}^2$ is trivial, then $W = \mathrm{id}$ on R.*

Proof. It is proved in a more general form in [16]. □

The next theorem (due to Serre) gives a practical criterion for the regularity of the subring R^W of the W-invariants of R. We state the theorem in its full generality, then apply it in our specific

situation. Recall that an invertible linear transformation σ of a finite dimensional vector space is called a pseudo-reflection if $\operatorname{rank}(1-\sigma) \leqslant 1$.

Theorem 1. *(See Serre [4,16].) Let A be a noetherian regular local ring with maximal ideal $\mathfrak{m}$ and residue field k. Let G be a finite group of automorphisms of A, and let A^G denote the local ring of G-invariants of A. Suppose that*:

(1) *the characteristic of k does not divide the order of G,*
(2) *G acts trivially on k,*
(3) *A is a finitely generated A^G-module.*

Then A^G is regular if and only if the image of G in $\operatorname{Aut}_k(\mathfrak{m}/\mathfrak{m}^2)$ is generated by pseudo-reflections.

Applying the above Serre's theorem to our situation we get the following result.

Lemma 2.2. *Let x, y be a regular system of parameters of R. Suppose the set of two minimal prime ideals $\{(x), (y)\}$ is stable under W, then there are four cases*:

(a) $W(x) = u_x x$, $W(y) = u_y y$, *such that* $u_x \equiv u_y \equiv 1 \pmod{\mathfrak{m}}$, *then* $W = \mathrm{id}$,
(b) $W(x) = u_x x$, $W(y) = u_y y$, *such that* $u_x \equiv -u_y \equiv \pm 1 \pmod{\mathfrak{m}}$, *then* R^W *is regular,*
(c) $W(x) = u_x x$, $W(y) = u_y y$, *such that* $u_x \equiv u_y \equiv -1 \pmod{\mathfrak{m}}$, *then* R^W *is non-regular,*
(d) $W(x) = u_x y$, $W(y) = u_y x$, *then* R^W *is regular.*

In the above u_x and u_y are units of R.

Proof. Since W fixes the set $\{(x), (y)\}$, there are two possibilities. We first assume $W((x)) = (x)$ and $W((y)) = (y)$, that is $W(x) = u_x x$ and $W(y) = u_y y$ for $u_x, u_y \in R^\times$. As $W^2(x) = W(u_x)W(x) = W(u_x)u_x x = x$ we get $W(u_x)u_x = 1$. By the assumption $W(u_x) \equiv u_x \pmod{\mathfrak{m}}$, which implies that $u_x \equiv \pm 1 \pmod{\mathfrak{m}}$, so we get the first three cases.

To study the regularity of the invariant ring in each case we proceed as follows. In case (a), let $x' = x + W(x)$, $y' = y + W(y)$. Since $p \neq 2$ the elements x' and y' are again a regular system of parameters for R. And $W(x') = x'$ and $W(y') = y'$, which implies W is trivial by Lemma 2.1. In case (b), let $x' = x \pm W(x)$ and $y' = y \mp W(y)$, respectively, then they again form a regular system of parameters, such that $W(x') = \pm x'$ and $W(y') = \mp y'$, respectively. So W is a pseudo-reflection, and by Theorem 1 the invariant ring R^W is regular. In case (c), let $x' = x - W(x)$ and $y' = y - W(y)$, then $W(x') = -x'$ and $W(y') = -y'$, i.e. W is not a pseudo-reflection. Therefore R^W is non-regular.

We now assume W exchanges the two minimal prime ideals (x) and (y), so we are in case (d). This time we write $s = x + W(x)$ and $t = x - W(x)$, then s and t are regular parameters for R, and $W(s) = s$, $W(t) = -t$. Again, by Theorem 1 we conclude that R^W is regular. □

Remark 2.1. Lemma 2.2 usually applies to the following geometric setting. Let us assume the two local parameters x and y correspond to two local closed subschemes through the closed point of a regular local scheme $\operatorname{Spec} R$. Suppose an involution W fixes the regular point and preserves the two local subschemes. Case (a) happens when W acts trivially on both subschemes. Case (b) shows up when W acts trivially on one subscheme and non-trivially on the other one. Case (c) happens when W acts non-trivially on both subschemes. Case (d) corresponds to the case in which W interchanges the two local subschemes.

Let $Y = \operatorname{Spec} R$ and $Y^W = \operatorname{Spec} R^W$ be the quotient local scheme. We know that only in case 2.2(c) Y^W is a non-regular local scheme. In this case the minimal resolution of Y^W can be accomplished as

follows. Let $\widetilde{Y} = \mathrm{Proj}(\sum_{n\geqslant 0}\mathfrak{m}^n)$ be the blowing up of Y at the closed point corresponding to $\mathfrak{m}$. By [8, IV Proposition 19.4.11] the scheme $\widetilde{Y}$ is covered by two open affines

$$D_+(u) = \mathrm{Spec}\, R[u]/(x-uy), \qquad D_+(v) = \mathrm{Spec}\, R[v]/(y-vy).$$

The exceptional curve of the blowing-up $\widetilde{Y} \xrightarrow{\pi} Y$ is isomorphic to $\mathbb{P}^1_k$ and is given by $y=0$ and $x=0$ on $D_+(u)$ and $D_+(v)$ respectively, where x and y are any regular parameters of R. As seen in Lemma 2.2 after change of coordinates we may assume that $W(x) = -x$ and $W(y) = -y$. The action of W extends naturally onto $\widetilde{Y}$, and is given explicitly by $W(x) = -x, W(y) = -y, W(u) = u$. This time W has no fixed points of case 2.2(c) on $\widetilde{Y}$, hence the quotient $\widetilde{Y}/W$ is regular and is the minimal resolution of $\mathrm{Spec}\, R^W$.

Now we turn to the specific situation of $X_0(N)$, or more precisely the moduli stack $[\Gamma_0(N)]$. To apply Lemma 2.2 we need to find a regular system of parameters for the complete local ring $\widehat{\mathcal{O}}_{[\Gamma_0(N)],P}$ at a geometric point $P = (E_1 \to E_2)$. If P is supersingular, such a system is found in [11, Proposition 7.8.2]. If P is ordinary, the system is not explicitly proved in [11]. In the following we will make it explicit. Such a system is already used in [4] (without proof) to derive the explicit local equations of $[\Gamma_0(N)]$.

To begin with we recall that the local universal formal deformation ring of an elliptic curve E_k is isomorphic to $W(k)[[T]]$, where $W(k)$ is the ring of Witt vectors over k. If E is supersingular the parameter T represents the equi-characteristic deformation of E. If E is ordinary then $T = q-1$ with q the Serre–Tate parameter of E [10]. In the following lemma we use T_i to denote the T-invariant for E_i.

Lemma 2.3. *Let $P = [(E_1 \xrightarrow{\varphi} E_2)]$ be a k-rational point of $[\Gamma_0(p^n)]$ with $n \geqslant 1$. Suppose that either E_1 is supersingular or when E_1 is ordinary φ is of type (a,b) for $a, b \geqslant 1$, then T_1 and T_2 form a regular system of parameters for the complete local ring of $[\Gamma_0(p^n)]$ at P.*

Proof. As mentioned above, when E_1 is supersingular the claim is Proposition 7.8.2 in [11]. So we assume that E_1 is ordinary. Following [11, Theorem 5.3.2] we just need to show the following moduli-theoretic rigidity property:

Let R be a local artinian $W(k)$-algebra with residue field k. Let $E'_1 \xrightarrow{\varphi'} E'_2$ be a cyclic isogeny over R that is a formal deformation of $E_1 \xrightarrow{\varphi} E_2$. If $q(E'_1) = q(E'_2) = 1$, then R is a k-algebra and $E'_1 \to E'_2$ is a constant deformation.

By the assumption that $q(E'_1) = q(E'_2) = 1$ we may assume that p-divisible groups of E'_1 and E'_2 split, that is E'_1 and E'_2 are the Serre–Tate canonical lift of E_1 and E_2 to R respectively, see [10, Section 2]. So we have [10]

$$\mathrm{Hom}_R\big(E'_1, E'_2\big) \cong \mathrm{Hom}_k(E_1, E_2), \tag{2.1}$$

where the isomorphism is induced by the reduction $R \to k$. By our assumption the isogeny $\varphi : E_1 \to E_2$ has a standard factorization

$$E_1 \xrightarrow{F^a} E_1^{(p^a)} \cong E_2^{(p^b)} \xrightarrow{V^b} E_2.$$

As $p = FV \in \mathrm{Hom}(E_1^{p^{a-1}}, E_2^{p^{b-1}} \cong E_1^{p^{a-1}})$ (note here we have used the assumption that $a, b \geqslant 1$), we get a decomposition $\varphi = p\psi$ for some $\psi \in \mathrm{Hom}_k(E_1, E_2)$, which induces through (2.1) a decomposition $\varphi' = p\psi'$ for φ'. So $E'_1[p] \subseteq \ker(\varphi')$, and $E'_1[p]$ is cyclic as a subgroup of the cyclic group $\ker(\varphi')$. By [11, Corollary 12.2.6] the cyclicity of $E'_1[p]$ implies that $p = 0 \in R$. Now the vanishing of p and T together implies that E_R and E'_R are constant, so is the isogeny between them. □

Remark 2.2.

(1) Since the moduli stack $[\Gamma_0(p^nN')]$ is étale over the moduli stack $[\Gamma_0(p^n)]$ (over $W(k)$), the above two parameters also give a regular system of parameters for the complete local ring of $[\Gamma_0(N)]$ by viewing $P = (E, C_{p^n}, C_{N'})$ as $(E, C_{N'}) \xrightarrow{\varphi} (E', C'_{N'})$ for $E' = E/C_{p^n}$ and $C'_{N'} = (C_{N'} + C_{p^n})/C_{p^n}$.
(2) The pair (T_1, T_2) does not form a regular system of parameters at ordinary points of type $(1,0)$ or $(0,1)$. However, $X_0(N)$ is smooth at ordinary points of type $(1,0)$ or $(0,1)$. So the result on [11, p. 508] implies that the quotient $X_0^M(N)$ is also smooth at ordinary points of type $(1,0)$ or $(0,1)$.

3. Determination of fixed points of W_M

In this section we determine the geometric points of $X_0(N)(\overline{\mathbb{F}}_p)$ whose images on $X_0^M(N)$ are singular. Let $P \in X_0(N)(\overline{\mathbb{F}}_p)$ be such a point. Then there are two possibilities for P: either $W_M(P) = P$, or $W_M(P) \neq P$ but P is singular on $X_0(N)$. It is obvious that in the second case the quotient $\overline{P}$ is singular on $X_0^M(N)$, so we will concentrate on the first case in the following. Recall that we assume: $v_2(N) \neq 1, 2$ and $v_3(N) \neq 1$.

3.1. Cuspidal fixed points

First let P be a cusp. It is already known [4] that P is a regular point of $X_0(N)$. Therefore, to study the regularity of its quotient $\overline{P}$ we may concentrate on fixed cusps of W_M.

Proposition 3.1. *If P is a cusp, then the image $\overline{P}$ of P on the quotient $X_0^M(N)$ is regular.*

Proof. Let $P \in X_0(N)(\overline{\mathbb{F}}_p)$ be a cusp fixed by W_M. As before let M' and N' be the part of M and N that is relatively prime to p, respectively. Note that the (reduced) (a,b)-component containing P is isomorphic to $X_0(N')_{\mathbb{F}_p}$ [4]. Under this identification the induced action of W_M on it is exactly $W_{M'}$. By [13, Proposition 3] (and that $M' \neq 4$, by the assumption on N) the involution $W_{M'}$ has no fixed points at cusps except when $M' = 1$. Now let us assume $M' = 1$, i.e. $M = p^n$. In this case, the fixed cusp P is on the (a,a)-component, and W_{p^n} acts trivially on the whole (a,a)-component. By Lemma 2.2 we conclude that $X_0^M(N)$ is regular at $\overline{P}$. □

3.2. Non-cuspidal fixed points

Now let $P \in Y_0(N)(\overline{\mathbb{F}}_p)$ be a non-cuspidal point fixed by W_M. We will study the singularity of $\overline{P}$ according to the following four cases depending on possible values of M, where as usual $n \geqslant 1$:

(1) $p \nmid M$,
(2) $M = p^n$,
(3) $M = p^nM'$, $M' \neq 1$ and $M \neq N$,
(4) $M = N = p^nN'$ and $N' \neq 1$.

Proposition 3.2. *In cases* (2), (3) *and* (4), *if $P \in \operatorname{Reg} X_0(N)$ is fixed by W_M then $\overline{P}$ is regular.*

Proof. In these cases W_{p^n} interchanges the source and target parameters at P (Lemma 2.3 and Remark 2.2), and $W_{M'}$ fixes each of them. Hence their product W_M interchanges the local parameters. So the quotient point $\overline{P}$ is regular by case (d) of Lemma 2.2. □

Proposition 3.3. *In case* (1), *if the W_M-fixed point P is in* $\operatorname{Reg} X_0(N)$ *and P is on the (a,b)-component for $a, b \geqslant 1$, then $\overline{P} \in \operatorname{Sing} X_0^M(N)$.*

Proof. The involution W_M preserves and acts non-trivially on each of the two parameters. By Lemma 2.2 case (c) or Remark 2.1 the proof is complete. □

Suppose $E_{\bar{\mathbb{F}}_p}$ has an extra automorphism $\tau \neq \pm 1$. It is well known that $\mathbb{Z}[\tau] \cong \mathbb{Z}[i]$ when $j(E) = 1728$ or $\mathbb{Z}[\omega]$ when $j(E) = 0$, where $i^2 = -1$ and $\omega^2 + \omega + 1 = 0$. We have the following result regarding the field of rationality of τ.

Lemma 3.4. *Let $E_{\mathbb{F}_p}$ be an elliptic curve with an extra automorphism $\tau \neq \pm 1$ with $p > 3$. Then τ is defined over $\mathbb{F}_p$ if and only if E is ordinary.*

Proof. We have the following explicit description of the extra automorphism τ. Suppose $j(E) = 0$, i.e. $\tau^6 = 1$. Without loss of generality we assume that τ is a generator of $\mathrm{Aut}(E)$. Then E has the following Weierstrass equation over $\bar{\mathbb{F}}_p$

$$y^2 = x^3 - 1$$

with $\tau(x) = \zeta^{-1}x$, $\tau(y) = -y$, where $\zeta \in \bar{\mathbb{F}}_p^{\times}$ is of exact order 3. It follows from these formulas that τ is defined over $\mathbb{F}_p$ iff $\zeta \in \mathbb{F}_p^{\times}$, which is equivalent to requiring $p \equiv 1 \pmod 3$. It is well known that $p \equiv 1 \pmod 3$ iff E is ordinary.

Suppose $j(E) = 1728$ and assume τ is a generator of $\mathrm{Aut}(E)$, then E is given by

$$y^2 = x^3 - x$$

with $\tau(x) = -x$, $\tau(y) = iy$, where $i \in \bar{\mathbb{F}}_p^{\times}$ is of exact order 4. This time τ is defined over $\mathbb{F}_p$ iff $i \in \mathbb{F}_p$, or equivalently $p \equiv 1 \pmod 4$. And it is well known that $p \equiv 1 \pmod 4$ iff E is ordinary. □

As a corollary of the above explicit computations we see that the induced action of the Frobenius on $\mathbb{Z}[\tau]$ is the complex conjugation if E is supersingular, and is trivial if E is ordinary.

Now, we let $S_{N'}(\tau) = \{P' = (E, C_{N'}) \in X_0(N')(\bar{\mathbb{F}}_p)\colon\ \tau \in \mathrm{Aut}(P')\}$ be the set of points with an extra automorphism τ, and assume that $S_{N'}(\tau)$ is non-empty. So $\tau \in \mathrm{Aut}(E)$ and $\tau(C_{N'}) = C_{N'}$. Let $N' = p_1^{e_1} \cdots p_s^{e_s}$ be the prime decomposition of N'. By [6] and the assumption that $v_2(N) \neq 1$, $v_3(N) \neq 1$, we know that p_i splits in $\mathbb{Q}(\tau)$, and we let $(p_i) = \mathfrak{p}_i\bar{\mathfrak{p}}_i$ be the decomposition of the ideal (p_i) in $\mathbb{Z}[\tau]$. Let S be the set of ideals of the form $\mathcal{N}' = \prod_i \mathfrak{q}_i^{e_i}$, where $\mathfrak{q}_i$ is either $\mathfrak{p}_i$ or $\bar{\mathfrak{p}}_i$ for each i. Since $\mathbb{Z}[\tau]$ has class number one each such ideal is principal, i.e. $\mathcal{N}' = (\mathcal{N}')$ for some element $\mathcal{N}' \in \mathbb{Z}[\tau]$. By [15] there is a natural one-to-one correspondence between S and $S_{N'}(\tau)$. For each $\mathcal{N}' \in S$, the point of $X_0(N')$ associated to $\mathcal{N}'$ corresponds to the endomorphism $(E \xrightarrow{\mathcal{N}'} E)$, where E is the unique elliptic curve having the extra automorphism τ. Under this correspondence the action of $W_{M'}$ on S is given by [6]

$$W_{M'} : \mathcal{N}' = \prod_{\mathfrak{q}_i | M'} \mathfrak{q}_i^{e_i} \cdot \prod_{\mathfrak{q}_i \nmid M'} \mathfrak{q}_i^{e_i} \mapsto \prod_{\mathfrak{q}_i | M'} \bar{\mathfrak{q}}_i^{e_i} \cdot \prod_{\mathfrak{q}_i \nmid M'} \mathfrak{q}_i^{e_i}.$$

From this description of $W_{M'}$ we easily get the following observation.

Lemma 3.5. *The following properties of $W_{M'}$ are true.*

(a) *$W_{M'}$ acts freely on S or $S_{N'}(\tau)$ for $M' \neq 1$;*
(b) *$W_{M'}$ has the same action as the complex conjugation on S iff $M' = N'$.*

Proposition 3.6. *In cases* (1) *and* (3)*, every W_M-fixed point P is in* $\mathrm{Reg}\, X_0(N)$.

Proof. Suppose $P = [(E, C_{N'}, C_{p^n})] \in \operatorname{Sing} X_0(N)$, then $P' = [(E, C_{N'})] \in S_{N'}(\tau)$ for an extra automorphism τ. By the above description $W_{M'}$ acts freely on $S_{N'}(\tau)$. Hence P in case (1) is not fixed by $W_M = W_{M'}$.

There are two possibilities in case (3). First let P be ordinary and $W_{p^n} W_{M'}(P) = P$. As W_{p^n} switches the (a, b)-component to the (b, a)-component of $X_0(N)$, so P must be on the (a, a)-component and $W_{p^n}(P) = P$ (n is even). Hence P' must be fixed by $W_{M'}$, which is impossible because the action of $W_{M'}$ on $S_{N'}(\tau)$ is free.

Now let P be supersingular and fixed by W_M. Then

$$W_{p^n}(P') = \left[\left(E/C_{p^n}, \left(C_{N'} + E\left[p^n\right]\right)/C_{p^n}\right)\right] = \begin{cases} P'^{(p)}, & \text{if } n \text{ is odd,} \\ P', & \text{if } n \text{ is even,} \end{cases}$$

where $P'^{(p)}$ is the image under the Frobenius of $P' \in X_0(N')$. As P is fixed by W_M, $W_{M'}(P'^{(p)}) = P'$ if n is odd, or $W_{M'}(P') = P'$ if n is even. Neither of these is possible due to Lemma 3.5.

Therefore we conclude that $P \in \operatorname{Reg} X_0(N)$. □

Proposition 3.7. *In case* (2)*, suppose* $P \in \operatorname{Sing} X_0(N)$*. Then*

(a) *if n is even then P is fixed by W_M iff P is on the (a, a)-component*;
(b) *if n is odd then P is fixed by W_M iff $N = M = p^n$. In this case P is supersingular.*

Proof. (a) is obvious. Let n be odd. If $P = [(E, C_{N'}, C_{p^n})]$ is fixed by W_M, then P is supersingular. As $W_M(P') = P'^{(p)}$, we get $P' = P'^{(p)}$, which is possible only if $N' = 1$ (as the Frobenius acts as the complex conjugation on $S_{N'}(\tau)$). The other direction follows easily. □

Proposition 3.8. *In case* (4) *and suppose* $P \in \operatorname{Sing} X_0(N)$*. Then P is fixed by W_M if and only if n is odd and P is supersingular.*

Proof. The proof is exactly the same as that of Proposition 3.6. The only difference is that $W_{M'}(P') = P'^{(p)}$ for $M' = N'$. □

3.3. Points on $X_0(N)$ with singular quotients

Summarizing the above arguments we obtain the following list of types of points on $X_0(N)$ that may have singular images on the quotient $X_0^M(N)$.

Type A: Non-W_M-fixed singular points on $X_0(N)$.
Type B: Regular fixed points of W_M for $p \nmid M$ on the (a, b)-component with $a, b \geqslant 1$ (Propositions 3.3 and 3.6).
Type C: Singular fixed point of W_M for $M = p^n$. They occur iff either $2|n$ or $2 \nmid n$ and $N = p^n$ (Proposition 3.7).
Type D: Singular fixed points of W_M for $M' \neq 1$. They are supersingular and occur iff $M = N$ and n is odd (Propositions 3.6 and 3.8).

We will also use the same type name to label the singular quotient on $X_0^M(N)$ of a point belonging to one of the above types.

4. Resolutions

We now resolve all possible singularities of $X_0^M(N)$ over $W(\overline{\mathbb{F}}_p)$ according to the types listed in the end of the last section. Readers may consult [12] for basic theories and facts on arithmetic curves.

4.1. Points of type A

These singularities are locally (in the étale topology) isomorphic to their pre-images in $X_0(N)$. Therefore their minimal resolutions are the same as the corresponding ones on $X_0(N)$, which can be found in [4]. We record them here for the sake of completeness. In each of the following figures the negative number denotes the self-intersection number of the corresponding $\mathbb{P}^1$-curve, and the positive number attached represents the curve's multiplicity in the special fiber. If $p \mid M$, we label components by pairs (a, b) with $a \geqslant b$ and $a + b = n$. If $p \nmid M$, we label the components by pairs (a, b) with $a + b = n$.

(A1) $j = 0$, ordinary, so $p \equiv 1 \pmod 3$, and P is on the (a, b)-component.

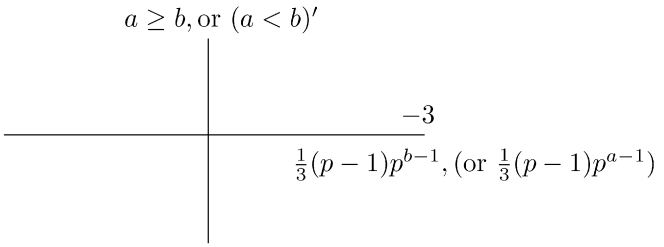

Fig. 1. $j = 0$, ordinary on (a, b)-component.

Note that the component with $a < b$ shows up only if $p \nmid M$, in which case $\widetilde{X}_0^M(N)_{\mathbb{F}_p}$ has $n + 1$ irreducible components. Otherwise $\widetilde{X}_0^M(N)_{\mathbb{F}_p}$ has $\lfloor \frac{n+1}{2} \rfloor$ components indexed by $a \geqslant b$ for W_{p^n} exchanges the (a, b) and (b, a)-components.

(A2) $j = 0$, supersingular, so $p \equiv -1 \pmod 3$, and $n = 2k$ is even.

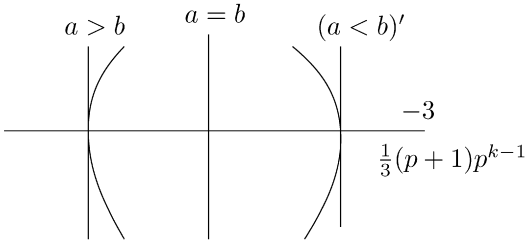

Fig. 2. $j = 0$, supersingular, $n = 2k$.

The label $(a < b)'$ here (and hereafter) means that this component exists only if $p \nmid M$.

(A3) $j = 0$, supersingular, i.e. $p \equiv -1 \pmod 3$, and $n = 2k + 1$.

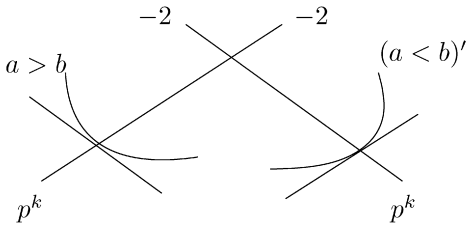

Fig. 3. $j = 0$, supersingular, $n = 2k + 1$.

(A4) $j = 1728$, ordinary, so $p \equiv 1 \pmod 4$.

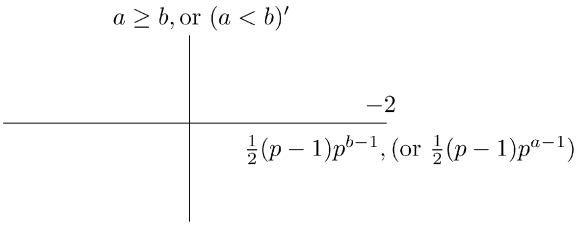

Fig. 4. $j = 1728$, ordinary on (a, b)-component.

Here similar to (A1), the component with $a < b$ shows up only if $p \nmid M$.

(A5) $j = 1728$, supersingular, so $p \equiv -1 \pmod 4$, and $n = 2k$.

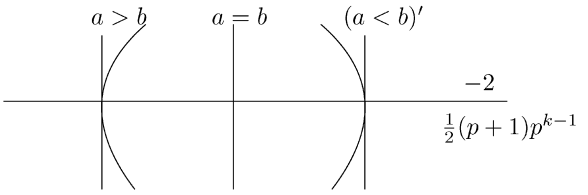

Fig. 5. $j = 1728$, supersingular, $n = 2k$.

(A6) $j = 1728$, supersingular, i.e. $p \equiv -1 \pmod 4$, and $n = 2k + 1$.

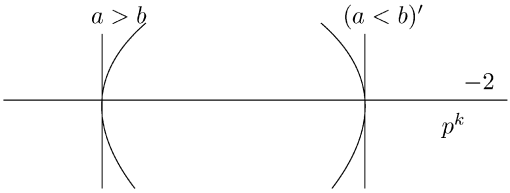

Fig. 6. $j = 1728$, supersingular, $n = 2k + 1$.

4.2. Points of type B

Let $p \nmid M$. The fixed points of W_M are regular on $X_0(N)$, and they are either all ordinary (when p splits in $\mathbb{Q}(\sqrt{-M})$) or all supersingular (when p is inert in $\mathbb{Q}(\sqrt{-M})$). The ordinary fixed points on the $(n, 0)$ or $(0, n)$-components produce regular quotients on $\widetilde{X_0(N)/W_M}$ [11, p. 508]. All other fixed points do produce singularities (Proposition 3.3), and can be resolved by one blowing up, see Section 2. We have the following figures. In each of the following figures, the first arrow means a blowing up and the second one means taking the quotient by W_M.

(B1) P is ordinary on the (a, b)-component with $a, b \geqslant 1$.

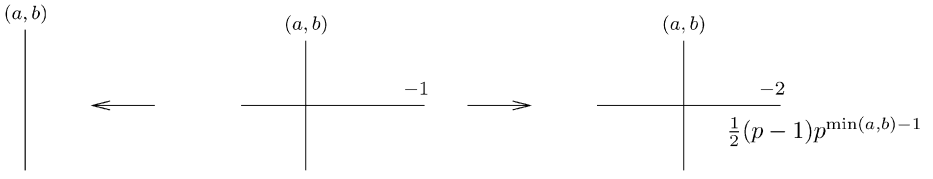

Fig. 7. j ordinary, $p \nmid M$, $a, b > 0$.

(B2) P is supersingular.

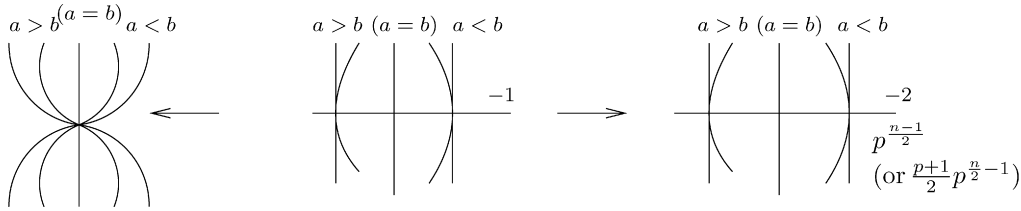

Fig. 8. j supersingular, $p \nmid M$.

Here $(a = b)$ means the possible (a, a)-component, which exists iff n is even. The intersection number between the (a_1, b_1) and (a_2, b_2)-components is $\frac{1}{2}(p^{a_2-b_2} - 1)$, where $a_i > b_i$ and $a_1 > a_2$. For $a_i < b_i$ and $a_1 > a_2$ the intersection number between the (a_1, b_1) and (a_2, b_2)-components is $\frac{1}{2}(p^{b_2-a_2} - 1)$.

To resolve singularities of the remaining types, we proceed as follows. We first describe the extended action W_M on the minimal resolution $\widetilde{X}_0(N)$ of $X_0(N)$. Then we locate and analyze the fixed points of W_M on $\widetilde{X}_0(N)$. At last we get the minimal resolution by taking the quotient of suitable blowing ups of $\widetilde{X}_0(N)$. The intersection numbers of local analytic branches are also computed. As before let $P \in X_0(N)$ be fixed by W_M with its quotient $\overline{P} \in \operatorname{Sing} X_0^M(N)$, and let $\pi : \widetilde{X}_0(N) \to X_0(N)$ be the minimal resolution constructed in [4].

4.3. Points of type C

In this case $M = p^n$. The induced action of W_M on the exceptional divisor $\pi^{-1}(P)$ and the minimal resolution can be described case by case as follows.

(C1) $j = 0$, is ordinary (that is $p \equiv 1 \pmod 3$). So $n = 2k$ is even.

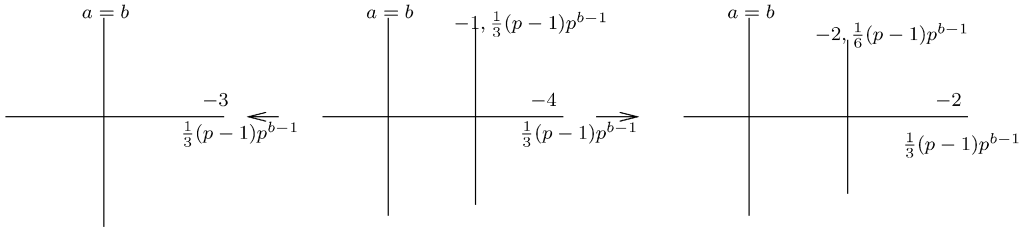

Fig. 9. $j = 0$, ordinary and $a = b$.

Here the leftmost graph describes the special fiber of the resolution $\widetilde{X}_0(N)$ around P. The horizontal line denotes the exceptional $\mathbb{P}^1$-curve $\pi^{-1}(P)$. The involution W_{p^n} has two fixed points on $\pi^{-1}(P)$, one of which is its intersection with the (k, k)-component. The graph in the middle is obtained from the left one by blowing up the other fixed point of W_{p^n} on $\pi^{-1}(P)$. Such a blowing up is needed because the other fixed point does produce a singular point on $\widetilde{X}_0(N)/W_M$. Suppose on the contrary that the quotient is regular. Let C be the image of $\widetilde{C} = \pi^{-1}(P)$, then $\pi_M^*(C) = \widetilde{C}$, where $\pi_M : \widetilde{X}_0(N) \to \widetilde{X}_0(N)/W_M$ is the quotient morphism. Comparing the intersection numbers we get

$$2C^2 = \pi_M^*(C) \cdot \pi_M^*(C) = \widetilde{C} \cdot \widetilde{C} = -3,$$

which is a contradiction. Therefore the quotient of the other fixed point on $\pi^{-1}(P)$ is singular.

From Section 2 we know such a singularity can be resolved by one blowing up, which is the first arrow of the above figure. The second arrow represents taking the regular quotient. So, the rightmost

graph is the graph of the special fiber of the minimal resolution $\widetilde{X}_0^M(N)$ of $\overline{P}$. The local intersection number between different reduced components is 1.

(C2) $j = 0$, supersingular ($p \equiv -1 \pmod 3$), and $n = 2k$.

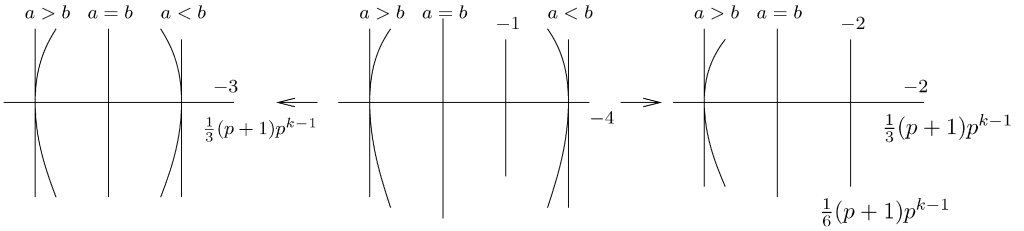

Fig. 10. $j = 0$, supersingular and $n = 2k$.

Similar to (B1), the leftmost graph is for $\widetilde{X}_0(N)_{\mathbb{F}_p}$. The middle one is the blowing up of $\widetilde{X}_0(N)$ at the other fixed point of W_{p^n} on $\pi^{-1}(P)$. The rightmost graph is the minimal resolution of $X_0^M(N)$ at $\overline{P}$.

The intersection number between the (a, b)-component and the horizontal (-2)-curve is 1. The intersection number between (a_1, b_1) and (a_2, b_2)-components $(a_1 > a_2)$ is $\frac{1}{3}(p^{a_2-b_2} - 1)$.

(C3) $j = 0$, supersingular ($p \equiv -1 \pmod 3$), and $n = 2k + 1$. So $M = N = p^n$.

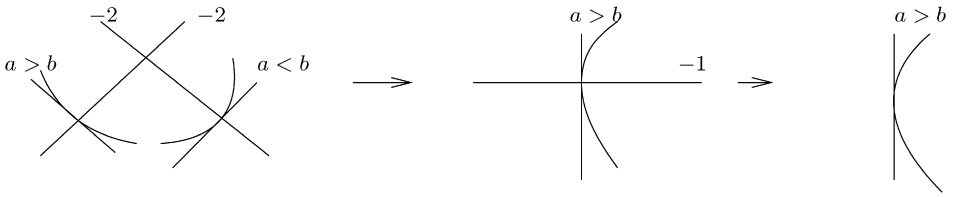

Fig. 11. $j = 0$, supersingular, $n = 2k + 1$.

The intersection of the two (-2)-$\mathbb{P}^1$'s, denoted by C_1 and C_2 respectively, is the only fixed point of W_M on $\pi^{-1}(P)$. Its image on the quotient $\widetilde{X}_0(N)/W_M$ is regular by Lemma 2.2. The first arrow denotes the quotient morphism $\pi_M : \widetilde{X}_0(N) \to \widetilde{X}_0(N)/W_M$. Let $C = \pi_M(C_1) = \pi_M(C_2)$ be the horizontal line of the middle graph, then

$$2C^2 = \pi_M^*(C)^2 = (C_1 + C_2)^2 = -2.$$

Hence $C^2 = -1$. The rightmost graph is the minimal resolution obtained by blowing down the -1-curve C. Each reduced local irreducible component remains smooth after the blowing down because its intersection number with the (-1)-curve is 1.

The intersection number between the (a_1, b_1) and (a_2, b_2)-components is $\frac{1}{3}(p^{a_2-b_2}+1)$ for $a_1 > a_2$.

(C4) $j = 1728$, ordinary ($p \equiv 1 \pmod 4$). Hence $n = 2k$.

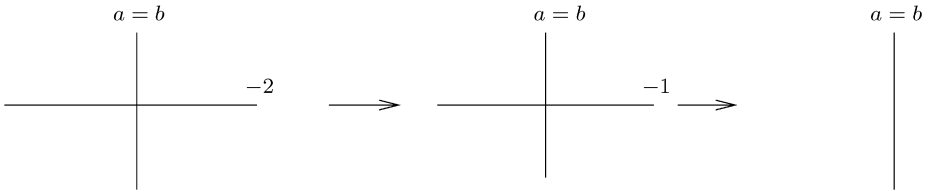

Fig. 12. $j = 1728$, ordinary, $n = 2k$.

The other fixed point of W_M on the exceptional (-2)-curve does not produce a quotient singularity. If it does, then a blowing up of it will have regular image on the quotient. But the strict pre-image of the (-2) curve on the blowing up will have self-intersection number -3. So the self-intersection number of its quotient is $-3/2$, which is absurd.

(C5) $j = 1728$, supersingular, i.e. $p \equiv -1 \pmod 4$, and $n = 2k$.

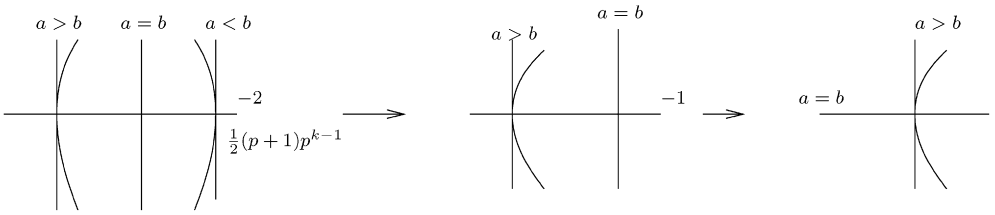

Fig. 13. $j = 1728$, supersingular, $n = 2k$.

An argument similar to that in (C4) shows that no blowing up is needed.

The intersection number between the (a_1, b_1) and (a_2, b_2)-components is $\frac{1}{2}(p^{a_2-b_2}+1)$.

(C6) $j = 1728$, supersingular, i.e. $p \equiv -1 \pmod 4$, and $n = 2k+1$. So $M = N = p^n$.

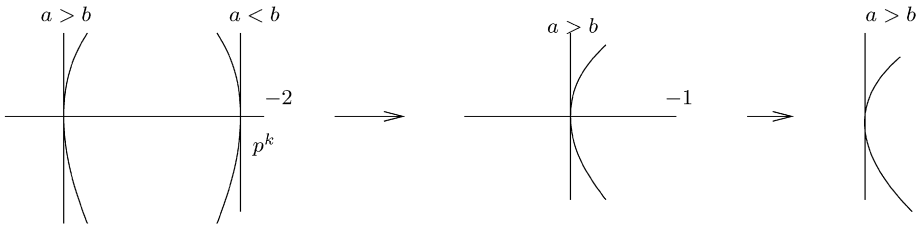

Fig. 14. $j = 1728$, supersingular, $n = 2k+1$.

In this case neither of the two fixed points on $\pi^{-1}(P)$ produces a singular quotient. Suppose (at least) one of them does, then we need to blow it up once to get a regular quotient. The exceptional (-1)-curve has multiplicity p^k. Since the action of W_{p^n} on it is trivial, its quotient should have multiplicity $p^k/2$, which is impossible.

The intersection number between the (a_1, b_1) and (a_2, b_2)-components is $\frac{1}{2}(p^{a_2-b_2}+1)$.

4.4. Points of type D

In this case $n = 2k+1$, $M = N$ and $N' = N/p^n \neq 1$. All points are supersingular. In each of the following figures the first arrow denotes the quotient morphism by W_M, and the second arrow denotes a blowing down.

(D1) $j = 0$ is supersingular, i.e. $p \equiv -1 \pmod 3$. This case is similar to (C3).

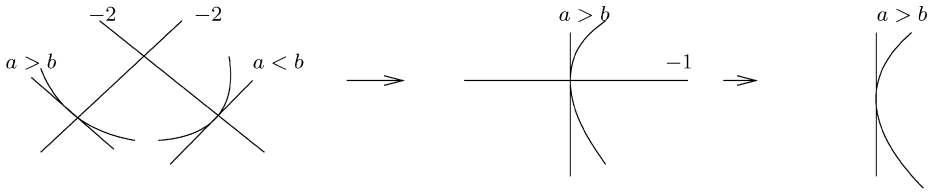

Fig. 15. $j = 0$, $M = N$, $n = 2k+1$.

The intersection number between the (a_1, b_1) and (a_2, b_2)-components for $a_1 > a_2$ is $\frac{1}{3}(p^{a_2-b_2}+1)$.

(D2) $j = 1728$, and $p \equiv -1 \pmod 4$. This is similar to (C6).

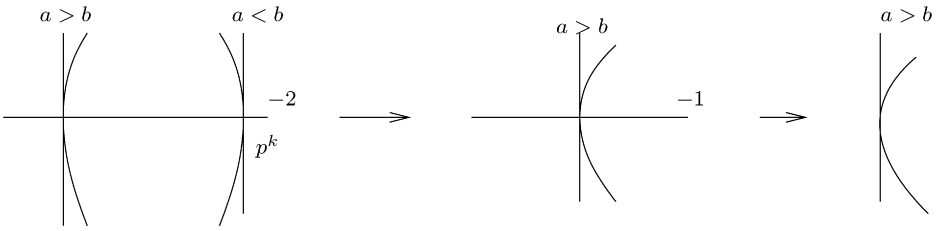

Fig. 16. $j = 1728$, $M = N$, $n = 2k+1$.

The intersection number between the (a_1, b_1) and (a_2, b_2)-components for $a_1 > a_2$ is $\frac{1}{2}(p^{a_2-b_2}+1)$.

5. Global graph of $\widetilde{X}_0^M(N)_{\overline{\mathbb{F}}_p}$

Similar to [4, Section 1.4] we now give a description of the global graph of the special fiber $\widetilde{X}_0^M(N)_{\overline{\mathbb{F}}_p}$, that is we will give its irreducible components, their multiplicities and their local intersection numbers. In the following we divide the problem into three different cases. In each case we describe step by step how to get the global graph of $\widetilde{X}_0^M(N)_{\overline{\mathbb{F}}_p}$.

5.1. $n = 2k+1$ and $p \mid M$

Step 1. Let $X_0^{M'}(N') = X_0(N')/W_{M'}$ be the quotient curve over $\mathbb{F}_p$. For each non-$\mathbb{F}_p$-rational supersingular $P \in X_0^{M'}(N')$ (which is the image of a supersingular point of $X_0(N')$, denoted again by P, such that $W_{M'}(P) \neq P^{(p)}$), we identify it with its Frobenius $P^{(p)}$, and make the resulting point a node of a new curve, which is denoted by C. Hence there is a natural birational morphism $X_0^{M'}(N') \to C$ which is two to one over the nodes of C and an isomorphism over smooth points of C.

Step 2. Now take $k+1$ copies of such C, indexed by (a, b) with $a > b$ and $a + b = n$. Let Φ be the projection morphism

$$\Phi : \coprod_{a+b=n, a>b} C_{a,b} \to C.$$

The (a, b)-component $C_{a,b}$ is given the multiplicity $\phi(p^b) = p^{b-1}(p-1)$.

Step 3. Glue these $k+1$ copies by contracting $\Phi^{-1}(P)$ to one point at every supersingular point P. There are two cases. First, suppose P is a regular point of C. Then at the contracted point there are $k+1$ reduced local analytic branches, denoted by $C_{a,b}^P$, one for each global $C_{a,b}$. The local intersection number between C_{a_1,b_1}^P and C_{a_2,b_2}^P is $p^{a_2-b_2}+1$ for $a_1 > a_2$.

If P is a node of C, then at the contracted point there are $n+1$ reduced local analytic branches, denoted by $C_{a,b}^P$ and $C_{a,b}^{P'}$, coming in pair from the global components $C_{a,b}$. The intersection number between C_{a_1,b_1}^P and $C_{a_2,b_2}^{P'}$ is 1, while the intersection number between C_{a_1,b_1}^P (resp. $C_{a_1,b_1}^{P'}$) and C_{a_2,b_2}^P (resp. $C_{a_2,b_2}^{P'}$) is $p^{a_2-b_2}$.

Step 4. Let $P' \in X_0(N')(\overline{\mathbb{F}}_p)$ be a point with $\mathrm{Aut}(P') \cong \mathbb{Z}/6\mathbb{Z}$ (so $j = 0$) such that $W_{M'}(P') = P'^{(p)}$, which happens iff $M = N$ and P' is supersingular. Then replace the unique point over P (henceforth P always means the image of P' on C) with the rightmost graph of Fig. 15.

Step 4′. Let P' be a point with $\mathrm{Aut}(P') \cong \mathbb{Z}/6\mathbb{Z}$ such that $W_{M'}(P') \neq P'^{(p)}$. If P' is ordinary let $\{P_{a,b}\} = \Phi^{-1}(P)$, and replace each $P_{a,b}$ for $b > 0$ with Fig. 1. If P' is supersingular then replace the unique point over P with Fig. 3.

Step 5. Let P' be a point with $\mathrm{Aut}(P') \cong \mathbb{Z}/4\mathbb{Z}$ ($j = 1728$) such that $W_{M'}(P') = P'^{(p)}$, which happens iff $M = N$ and P' is supersingular. Then replace the unique point over P with the rightmost graph of Fig. 16.

Step 5′. Let P' be a point with $\mathrm{Aut}(P') \cong \mathbb{Z}/4\mathbb{Z}$ such that $W_{M'}(P') \neq P'^{(p)}$. If P' is ordinary then replace $P_{a,b}$ for $b > 0$ with Fig. 4. If P' is supersingular then replace the unique point over P with Fig. 6.

5.2. $n = 2k$ and $p \mid M$

Step 1. Let $C = X_0^{M'}(N') = X_0(N')/W_{M'}$ be the quotient curve over $\mathbb{F}_p$. Take $k+1$ copies of C, indexed by (a, b) with $a \geqslant b$ and $a + b = n$. Let Φ be the projection morphism

$$\Phi : \coprod_{a+b=n, a\geqslant b} C_{a,b} \to C.$$

And the (a, b)-component $C_{a,b}$ is given the multiplicity $\phi(p^b)$, except that when $M = N = p^n$ the multiplicity of $C_{k,k}$ is given by $\frac{1}{2}\phi(p^k)$.

Step 2. Glue these $k+1$ copies by contracting $\Phi^{-1}(P)$ to one point at every supersingular point P. At such point there are $k+1$ local analytic branches, denoted by $C_{a,b}^P$, one for each global component $C_{a,b}$. The local intersection number between the local branches C_{a_1,b_1}^P and C_{a_2,b_2}^P is $p^{a_2-b_2} + 1$ for $a_1 > a_2$.

Step 3. Let $P' \in X_0(N')(\overline{\mathbb{F}}_p)$ be a point with $\mathrm{Aut}(P') \cong \mathbb{Z}/6\mathbb{Z}$ ($j = 0$) such that $W_{M'}(P') = P'$, which occurs iff $M = N = p^n$. If P' is ordinary let $\{P_{a,b}\} = \Phi^{-1}(P)$, then replace $P_{k,k}$ with the rightmost graph of Fig. 9 and replace $P_{a,b}$ for $a > b > 0$ with Fig. 1. If P' is supersingular then replace the unique point over P with the rightmost graph of Fig. 10.

Step 3′. Let P' be a point with $\mathrm{Aut}(P) \cong \mathbb{Z}/6\mathbb{Z}$ ($j = 0$) such that $W_{M'}(P') \neq P'$. If P' is ordinary replace $P_{a,b}$ for $b > 0$ with Fig. 1. If P is supersingular replace the unique point over P with Fig. 2.

Step 4. Let P' be a point $\mathrm{Aut}(P) \cong \mathbb{Z}/4\mathbb{Z}$ ($j = 1728$) such that $W_{M'}(P') = P'$, which occurs iff $M = N = p^n$. If P' is ordinary then replace $P_{k,k}$ with Fig. 4, and replace $P_{a,b}$ for $a > b > 0$ with the rightmost graph of Fig. 12. If P' is supersingular then replace the unique point over P with the rightmost graph of Fig. 13.

Step 4′. Let P' be a point $\mathrm{Aut}(P') \cong \mathbb{Z}/4\mathbb{Z}$ ($j = 1728$) such that $W_{M'}(P') \neq P'$. If P' is ordinary then replace $P_{a,b}$ for $b > 0$ with Fig. 4. If P' is supersingular replace the unique point over P with the rightmost graph of Fig. 5.

5.3. $p \nmid M$

Step 1. Let $C = X_0^M(N') = X_0(N')/W_M$ be the quotient curve over $\mathbb{F}_p$. Take $n+1$ copies of C, indexed by (a, b) with $a + b = n$. Let Φ be the morphism

$$\Phi : \coprod_{a+b=n} C_{a,b} \to C$$

given by the identity morphism if $a \geqslant b$ and by Frob^{b-a} if $a < b$, here Frob is the Frobenius morphism from C to C. The multiplicity of $C_{a,b}$ is given by $\phi(p^{\min(a,b)})$.

Step 2. Glue these $n+1$ copies of C by contracting $\Phi^{-1}(P)$ to one point at every supersingular point P. Let $C_{a,b}^P$ be the $n+1$ local branches at this point. This time the local equation at this point is

$$\left(x^{p^n} - y\right)\left(x - y^{p^n}\right) \prod_{a,b>0} \left(x^{p^{a-1}} - y^{p^{b-1}}\right)^{p-1} = 0.$$

From which the local intersection numbers are easy to compute.

Step 3. Let $P' \in X_0(N')(\overline{\mathbb{F}}_p)$ be a point with $\mathrm{Aut}(P) \cong \mathbb{Z}/2\mathbb{Z}$ ($j \neq 0, 1728$), such that $W_M(P') = P'$. If P' is ordinary let $\{P_{a,b}\} = \Phi^{-1}(P)$, and replace $P_{a,b}$ for $a, b > 0$ with the rightmost graph of Fig. 7. If P' is supersingular then replace the unique point over P with the rightmost graph of Fig. 8.

Step 4. Let P' be a point with $\mathrm{Aut}(P) \cong \mathbb{Z}/6\mathbb{Z}$ ($j = 0$), so $W_M(P') \neq P'$. If P' is ordinary replace $P_{a,b}$ for $a, b > 0$ with Fig. 1. If P' is supersingular then replace the unique point over P with Fig. 2 provided n is even, or with Fig. 3 provided n is odd.

Step 5. Let P' be a point with $\mathrm{Aut}(P) \cong \mathbb{Z}/4\mathbb{Z}$ ($j = 1728$), so $W_M(P') \neq P'$. If P' is ordinary replace $P_{a,b}$ for $a, b > 0$ with Fig. 4. If P' is supersingular then replace the unique point over P with Fig. 5 provided n is even, or with Fig. 6 provided n is odd.

6. Graphs of $\widetilde{X}_0^p(p)$ and $\widetilde{X}_0^{p^2}(p^2)$

As an example, we work out the global graphs of $\widetilde{X}_0^M(N)_{\overline{\mathbb{F}}_p}$ for $M = N = p$ or p^2.

6.1. Graph of $\widetilde{X}_0^p(p)_{\overline{\mathbb{F}}_p}$

Let S_{p^2} be the number of supersingular j-invariants that are not in $\mathbb{F}_p$. Then the graph of $\widetilde{X}_0^p(p)_{\overline{\mathbb{F}}_p}$ is given by the following picture.

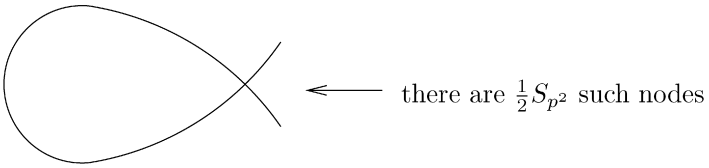

Fig. 17. $\widetilde{X}_0^p(p)_{\overline{\mathbb{F}}_p}$.

So $X_0^p(p)_{\overline{\mathbb{F}}_p}$ is a rational curve with $\frac{1}{2}S_{p^2}$ nodes.

6.2. Graph of $\widetilde{X}_0^{p^2}(p^2)$

There are four cases.

Case (a): $p = 12k + 1$. The number of supersingular j-invariants is k and $j = 0, 1728$ are ordinary.

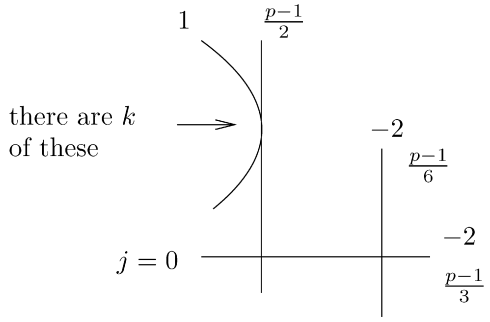

Fig. 18. $\widetilde{X}_0^{p^2}(p^2)_{\overline{\mathbb{F}}_p}$ for $p = 12k + 1$.

All irreducible components are $\mathbb{P}^1$. The long vertical line is the $(1, 1)$-component, and the curved one is the $(1, 0)$-component. The local intersection number at each of the k points is 2. All other intersection numbers are 1.

Case (b): $p = 12k + 5$. Then $j = 0$ is supersingular and $j = 1728$ is ordinary.

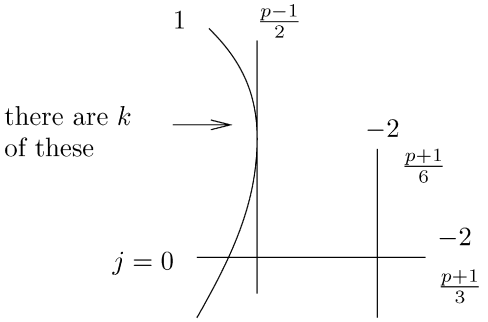

Fig. 19. $\widetilde{X}_0^{p^2}(p^2)_{\bar{\mathbb{F}}_p}$ for $p = 12k + 5$.

Case (c): $p = 12k + 7$. This time $j = 0$ is ordinary and $j = 1728$ is supersingular.

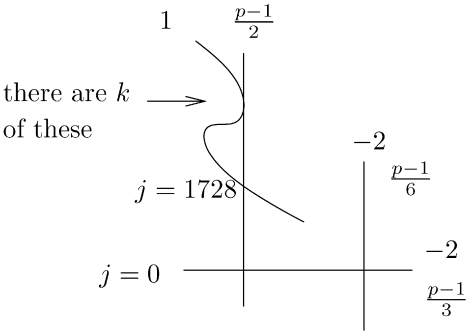

Fig. 20. $\widetilde{X}_0^{p^2}(p^2)_{\bar{\mathbb{F}}_p}$ for $p = 12k + 7$.

Case (d): $p = 12k + 11$. Both $j = 0$ and $j = 1728$ are supersingular.

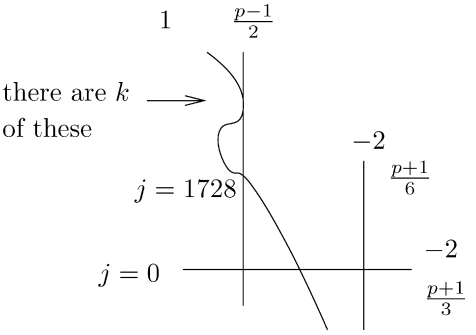

Fig. 21. $\widetilde{X}_0^{p^2}(p^2)_{\bar{\mathbb{F}}_p}$ for $p = 12k + 11$.

7. Applications

We present two arithmetic applications in this section. In the first application we give a new proof of the classic Deuring's formula on the number of $\mathbb{F}_p$-rational supersingular j-invariants. In the second application we study the action of Hecke operators on the component group of the Jacobian of $X_0^M(N)$ over $\mathbb{F}_p$.

7.1. Deuring's formula

Let S_p be the number of $\mathbb{F}_p$-rational supersingular j-invariants and let S_{p^2} be the number of remaining supersingular j-invariants (which are in $\mathbb{F}_{p^2}$ but not in $\mathbb{F}_p$). We have the following formula for S_p which is due to Deuring [3] (also see [1]), however our proof is different and is based on the minimal resolution of $X_0(N)/W_p$.

Theorem 2 *(Deuring). Let S_p be as above, then*

$$S_p = \begin{cases} \frac{1}{2}(h_p + h_{4p}) & \text{if } p \equiv 3 \pmod 4, \\ \frac{1}{2}h_{4p}, & \text{if } p \equiv 1 \pmod 4 \end{cases}$$

where h_d is the class number of the quadratic order of discriminant $-d$.

Proof. By Section 6 we know $\widetilde{X}_0^p(p)_{\bar{\mathbb{F}}_p}$ is a rational curve with $\frac{1}{2}S_{p^2}$ nodes, therefore

$$p_a\big(X_0^p(p)_{\mathbb{C}}\big) = p_a\big(\widetilde{X}_0^p(p)_{\bar{\mathbb{F}}_p}\big) = \frac{1}{2}S_{p^2}, \tag{7.1}$$

where $p_a(C)$ denotes the arithmetic genus of a curve C.

Recall the following well-known formula for $p_a(X_0(p)_{\mathbb{C}})$ [2, VI Théorème 6.9]

$$p_a\big(X_0(p)_{\mathbb{C}}\big) = S_p + S_{p^2} - 1. \tag{7.2}$$

Applying the Hurwitz formula to the double covering $X_0(p)_{\mathbb{C}} \to X_0^p(p)_{\mathbb{C}}$ we get

$$2\big[p_a\big(X_0(p)_{\mathbb{C}}\big) - 1\big] = 4\big[p_a\big(X_0^p(p)_{\mathbb{C}}\big) - 1\big] + H, \tag{7.3}$$

where the ramification index H is given by [13, p. 454]

$$H = \begin{cases} h_p + h_{4p}, & \text{if } p \equiv 3 \pmod 4, \\ h_{4p}, & \text{if } p \equiv 1 \pmod 4. \end{cases} \tag{7.4}$$

Now a manipulation of (7.1) through (7.4) concludes that $S_p = \frac{1}{2}H$. □

More generally, let $S_{N',p}$ be the number of $\mathbb{F}_p$-rational supersingular points on $X_0(N')(\bar{\mathbb{F}}_p)$, and let $N' = \prod_i q_i^{d_i}$ be the prime decomposition of N'. Then we have the following formula:

$$S_{N',p} = H \cdot \prod_i \left(1 + \left(\frac{-4p}{q_i}\right)\right), \tag{7.5}$$

where H is given by (7.4) and $(\frac{-4p}{q_i})$ is the usual Legendre symbol. The proof of (7.5) follows the same line and is left to interested readers.

7.2. Component group of $J_{X_0^M(N),\bar{\mathbb{F}}_p}$

Let l be a prime not dividing N. The Hecke operator T_l on $X_0(N)$ commutes with the involution W_M, hence induces a Hecke operator, denoted again by T_l, on the Atkin–Lehner quotient $X_0^M(N)$. More concretely, let

$$S : X_0(Nl) \to X_0(N), \qquad T : X_0(Nl) \to X_0(N)$$

be the two degeneration maps, defined by the natural maps $S : [(E, C_N, C_l)] \mapsto [(E, C_N)]$ and $T : [(E, C_N, C_l)] \mapsto [(E/C_l, (C_N + C_l)/C_l)]$ respectively. As they commute with W_M they induce maps on the quotients

$$S : X_0^M(Nl) \to X_0^M(N), \qquad T : X_0^M(Nl) \to X_0^M(N).$$

The Hecke operator T_l on the Jacobian $J_{X_0^M(N)}$ of $X_0^M(N)$ is then defined by

$$T_l = T_* S^*.$$

From now on we write $\Phi_{N,p}^M$ for the component group of the Néron model of $J_{X_0^M(N)}$ over $W(\bar{\mathbb{F}}_p)$. We will show the action of T_l on $\Phi_{N,p}^M$ is Eisenstein, i.e. $T_l = l + 1$, in the following simplest case. More cases and details will be included in a separate paper.

Theorem 3. *Suppose $p \mid M$, $M' \neq 1$ and if n is odd also assume $M' \neq N'$, then $T_l = l + 1$ on $\Phi_{N,p}^M$.*

Proof. By Section 3.3, the above assumptions imply that there are only singularities of Type A on $X_0(N)$ or $X_0(Nl)$, and $\pi_M(\operatorname{Sing} X_0(N)) = \operatorname{Sing} X_0^M(N)$. These two facts will be used in (7.7) and (7.10) respectively. Our proof follows closely the method used for $X_0(N)$ in [5] and [15].

Let us first recall (due to Raynaud [14]) how to compute the component group of the Jacobian of a general regular curve X/R, where R is a strictly Henselian DVR (in our situation $R = W(\bar{\mathbb{F}}_p)$). Let s and η be the closed and generic point of $\operatorname{Spec} R$ respectively. We write the free group of components

$$D(X) = \sum_C \mathbb{Z}[C]$$

where C range over all reduced irreducible components of the special fiber X_s. There is a natural endomorphism α of $D(X)$, which on each generator $[C']$ of $D(X)$ is given by

$$\alpha : [C'] \mapsto \sum_C (C' \cdot C)[C],$$

where $C' \cdot C$ is the intersection pairing on X [12]. Let deg be the total degree map defined by

$$\deg(C') = \sum_C m_C (C' \cdot C),$$

where $X_s = \sum_C m_C C$ is the special fiber. They give a complex

$$D(X) \xrightarrow{\alpha} D(X) \xrightarrow{\deg} \mathbb{Z}$$

whose cohomology is the component group of the Jacobian of X at p:

$$\Phi_p(X) = \ker(\deg)/\operatorname{im}(\alpha).$$

Let $\pi : X_R \to Y_R$ be a morphism between regular curves X and Y. Then π induces a map $\pi^*_{\deg}$: $D(Y) \to D(X)$ given by

$$\pi^*_{\deg}(C) = \sum_{C' \overset{\pi}{\mapsto} C} \deg(\pi|_{C'})[C'] \tag{7.6}$$

which induces $\pi^* : \Phi_p(Y) \to \Phi_p(X)$, see [5] for more information.

Similar to [5, Section 4.1] we get the following diagram associated to the degeneration map S

$$\begin{array}{ccc}
X_0(Nl)^{*S} & \xrightarrow{S} & X_0(N)^* \\
\downarrow{\scriptstyle \pi_M^S} & & \downarrow{\scriptstyle \pi_M} \\
X_0^M(Nl)^{*S} & \xrightarrow{S} & X_0^M(N)^* \\
\downarrow{\scriptstyle \pi^S} & & \downarrow{\scriptstyle \pi} \\
\widetilde{X}_0^M(Nl) & & \widetilde{X}_0^M(N) \\
\downarrow & & \downarrow \\
X_0^M(Nl) & \xrightarrow{S} & X_0^M(N)
\end{array} \tag{7.7}$$

Here the bottom S is the morphism induced by the degeneration map S from $X_0(Nl)$ to $X_0(N)$. The curve $X_0(N)^*$ is obtained by some blowing ups of $\widetilde{X}_0(N)$, and is the same as the $X_0(N)^*$ in [5]. The curve $X_0(Nl)^{*S}$ is the same as that in [5]. The top S-morphism is also the one used in [5]. By our assumptions W_M acts freely on $\operatorname{Sing} X_0(N)$ (resp. on $\operatorname{Sing} X_0(Nl)$), so W_M extends naturally onto $X_0(N)^*$ (resp. $X_0(Nl)^*$), and acts freely on the exceptional loci. Therefore, the quotient curves $X_0^M(N)^*$ and $X^M(Nl)^*$ are regular (as the only singularities are of Type A, and they are already resolved in $X_0(N)^*$ and $X_0(Nl)^{*S}$). The middle vertical morphism π (resp. π^S) consists of blowing downs that produce the minimal resolution $\widetilde{X}_0^M(N)$ (resp. $\widetilde{X}_0^M(Nl)$). The S-morphism on the second line is induced by the top S on the quotients.

Taking the free abelian groups on components of the middle square diagram we get

$$\begin{array}{ccc}
D_l^{S*} & \xleftarrow{S^*_{\deg}} & D^* \\
\downarrow{\scriptstyle \pi^{S*,-1}_{\deg}} & & \uparrow{\scriptstyle \pi^*_{\deg}} \\
\widetilde{D}_l & & \widetilde{D}
\end{array} \tag{7.8}$$

whose composition $S^* = \pi^{*S,-1}_{\deg} S^*_{\deg} \pi^*_{\deg} : \widetilde{D} \to \widetilde{D}_l$, induces the map

$$S^* : \Phi^M_{N,p} \to \Phi^M_{Nl,p}$$

Here the map $\pi^{*S,-1}_{\deg}$ is defined as in [5, 3.3]. A similar construction also applies to the degeneration map T.

One key observation of [15] is that to show T_l is Eisenstein it suffices to show

$$S^* = T^* : \widetilde{D} \to \widetilde{D}_l, \tag{7.9}$$

which will imply $T_l = T_* T^* = \deg T = l + 1$.

We will prove (7.9) using the decomposition (7.8). The group $\widetilde{D}$ consists of two parts: (a,b)-components of $\widetilde{X}_0^M(N)$, and exceptional curves on $\widetilde{X}_0^M(N)$. If C an irreducible (a,b)-component of $\widetilde{X}_0(N)$, then $S^*([C]) = T^*([C])$, both of which equal $(l+1)$ times the (a,b)-component of $\widetilde{X}_0^M(Nl)$ by (7.6).

Now let C_x be an exceptional component of $\widetilde{X}_0^M(N)$ whose image is $x \in \operatorname{Sing} X_0^M(N)$. By definition of $\pi_{\deg}^*$ we have $\pi_{\deg}^*([C_x]) = [\widetilde{C}_x]$, where $\widetilde{C}_x$ is the strict pre-image of C_x in $X_0^M(N)^*$. We also have

$$S_{\deg}^*\big([\widetilde{C}_x]\big) = \sum_{S(y)=x} \big[C_y^*\big]$$

where the sum is over the set $\{y \in X_0^M(Nl)(s):\ S(y) = x\}$, and C_y^* is the unique component of $X_0^M(Nl)^{*S}$ lying over y such that $S(C_y^*) = \widetilde{C}_x$. The coefficient of $[C_y^*]$ is 1 because $S : C_y^* \to \widetilde{C}_x$ has degree 1, see (7.6).

Hence we have

$$\begin{aligned} S^*\big([C_x]\big) &= \pi_{\deg}^{S*,-1} S_{\deg}^*\big([\widetilde{C}_x]\big) = \pi_{\deg}^{S*,-1}\Bigg(\sum_{S(y)=x} \big[C_y^*\big]\Bigg) \\ &= \pi_{\deg}^{S*,-1}\Bigg(\sum_{Sy=x,\ y\,\text{reg.}} \big[C_y^*\big]\Bigg) + \pi_{\deg}^{S*,-1}\Bigg(\sum_{Sy=x,\ y\,\text{sing.}} \big[C_y^*\big]\Bigg) \\ &= \pi_{\deg}^{S*,-1}\Bigg(\sum_{Sy=x,\ y\,\text{reg.}} \big[C_y^*\big]\Bigg) + \sum_{Sy=x,\ y\,\text{sing.}} [\widetilde{C}_y] \end{aligned}$$

where the first sum on the last line is over all components of $X_0^M(Nl)_s$ with $\widetilde{C}$ the strict pre-image of C in $\widetilde{X}_0^M(Nl)$, and the second sum is over $y \in \operatorname{Sing} X_0^M(Nl)$. The first part actually comes from blowing down of those exceptional curves in the pre-image of $y \in \operatorname{Reg} X_0(Nl)$. Similarly for T

$$\begin{aligned} T^*\big([C_x]\big) &= \pi_{\deg}^{T*,-1} T_{\deg}^*\big([\widetilde{C}_x]\big) \\ &= \pi_{\deg}^{T*,-1}\Bigg(\sum_{Ty=x,\ y\,\text{reg.}} \big[C_y^*\big]\Bigg) + \sum_{Ty=x,\ y\,\text{sing.}} [\widetilde{C}_y] \end{aligned}$$

By [5, 3.3] on the formula of blowing down we get

$$\pi_{\deg}^{S*,-1}\Bigg(\sum_{Sy=x,\ y\,\text{reg.}} \big[C_y^*\big]\Bigg) = \pi_{\deg}^{T*,-1}\Bigg(\sum_{Ty=x,\ y\,\text{reg.}} \big[C_y^*\big]\Bigg),$$

which is due to the fact that C_y^* and $C_{y'}^*$ are on the same (a,b)-component (the same label that x is on), and are formally isomorphic if $S(y) = S(y')$ or $T(y')$.

By [5, 4.2 Lemma 2] and the fact that $\pi_M(\operatorname{Sing} X_0(N)) = \operatorname{Sing} X_0^M(N)$ we have

$$\big\{y \in \operatorname{Sing} X_0^M(N):\ S(y) = x\big\} = \big\{y \in \operatorname{Sing} X_0^M(N):\ T(y) = x\big\}, \tag{7.10}$$

which implies

$$\sum_{Sy=x,\ y\,\text{sing.}} [\widetilde{C}_y] = \sum_{Ty=x,\ y\,\text{sing.}} [\widetilde{C}_y].$$

Therefore $S^* = T^*$ and the proof is complete. □

Note that (7.10) does not hold if $p \nmid M$ since there are Type B singularities, see Section 3. So if $p \nmid M$ the action of Hecke operators on the component group need not be Eisenstein.

Acknowledgments

We would like to thank the anonymous referee for many valuable advices and corrections.

References

[1] J. Brillhart, P. Morton, Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial, J. Number Theory 106 (1) (2004) 79–111.
[2] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II, in: Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, in: Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316.
[3] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272.
[4] B. Edixhoven, Minimal resolution and stable reduction of $X_0(N)$, Ann. Inst. Fourier (Grenoble) 40 (1) (1990) 31–67.
[5] B. Edixhoven, L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein", Astérisque (196–197) (1991) 7–8, Astérisque (1992) 159–170, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).
[6] B. Gross, Heegner points on $X_0(N)$, in: Modular Forms, Durham, 1983, in: Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.
[7] B. Gross, W. Kohnen, D. Zagier, Heegner points and derivatives of L-series. II, Math. Ann. 278 (1–4) (1987) 497–562.
[8] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV, Inst. Hautes Études Sci. Publ. Math. (32) (1967) 361.
[9] D. Jao, Supersingular primes for points on $X_0(p)/w_p$, J. Number Theory 113 (2) (2005) 208–225, MR MR2153276 (2006h:11057).
[10] N. Katz, Serre–Tate local moduli, in: Algebraic Surfaces, Orsay, 1976–1978, in: Lecture Notes in Math., vol. 868, Springer, Berlin, 1981, pp. 138–202.
[11] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Ann. of Math. Stud., vol. 108, Princeton Univ. Press, Princeton, NJ, 1985.
[12] Q. Liu, Algebraic Geometry and Arithmetic Curves, Oxf. Grad. Texts Math., vol. 6, Oxford Univ. Press, Oxford, 2002, translated from the French by Reinie Erné, Oxford Science Publications.
[13] A.P. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. France 102 (1974) 449–462.
[14] M. Raynaud, Spécialisation du foncteur de Picard, Inst. Hautes Études Sci. Publ. Math. (38) (1970) 27–76.
[15] K. Ribet, On the component groups and the Shimura subgroup of $J_0(N)$, in: Séminaire de Théorie des Nombres, Talence, 1987–1988, Univ. Bordeaux I, Talence, 1987–1988, pp. 1–10, Exp. No. 6.
[16] J. Watanabe, Some remarks on Cohen–Macaulay rings with many zero divisors and an application, J. Algebra 39 (1) (1976) 1–14.